PAR-15_RISKS

GESTION DES **RISQUES**

AMAURY ALRIQ
BILEL EL AMRANI
ROMÉO CAVAZZA

GESTION DES RISQUES

Ce document identifie, analyse et propose des plans de mitigation pour les risques majeurs du projet SmartFridge (iGloo). Il sert de référence pour le pilotage hebdomadaire. il définit pour chaque menace des plans de mitigation préventifs et des scénarios de contingence réactifs, garantissant ainsi la résilience du projet face aux aléas.

MATRICE DE CRITICITÉ

Chaque risque est évalué selon sa Probabilité (1=Rare à 5=Certain) et son Impact (1=Mineur à 5=Bloquant). *Score de Criticité = Probabilité x Impact*

ID	Domaine	Risque identifié	Prob.	Imp.	Score	Niveau
R1	Marché	Rejet du produit (Prix élevé, adoption faible)	**3**	**5**	**15**	**Critique**
R2	Technique	Défaillance Capteurs / Hardware	**4**	**4**	**16**	**Critique**
R3	Planning	Retard Livraison Prototype	**4**	**3**	**12**	**Majeur**
R4	Juridique	Non-conformité GDPR / Fuite de données	**2**	**5**	**10**	**Majeur**
R5	Humain	Problèmes de communication, force majeure	**3**	**2**	**6**	**Mineur**

Légende :

- **CRITIQUE** (Score > 15) : Action immédiate requise. Menace la viabilité du projet.
- **MAJEUR** (Score 10-14) : Surveillance rapprochée et plan de mitigation actif.
- **MINEUR** (Score < 10) : À surveiller périodiquement.

GESTION DE CRISE & PROCESSUS

En cas de matérialisation d'un risque critique (Score > 15) :

1. **Alerte :** Tout membre de l'équipe doit signaler immédiatement le problème au Chef de Projet.
2. **Cellule de Crise :** Réunion d'urgence (Chef de Projet + Tech Lead + Sponsor).
3. **Décision :** Activation du Plan de Contingence ou arrêt temporaire (Go/No-Go).
4. **Communication :** Information des parties prenantes (Board) sous 4h avec un plan d'action.

ANALYSE DÉTAILLÉE & PLANS D'ACTION

RISQUE MARCHÉ : REJET DU PRODUIT — Critique

Le prix final (> 2 000 €) est jugé trop élevé par le public cible (voir Persona Gérard), ou l'utilisation du scan manuel est considérée comme trop contraignante au quotidien. Ce risque aurait un impact direct sur les ventes et le retour sur investissement (ROI) et conduirait à l'échec commercial du projet.

En prévention :

- Réaliser des tests utilisateurs (UX Research) dès la phase POC pour valider l'acceptabilité.
- Prévoir une architecture modulaire permettant une version "Lite" (sans écran tactile) moins chère.

En réaction :

- Pivoter vers un modèle B2B (Cantines, Hôtels) ou proposer l'appareil en "Location longue durée".

RISQUE TECHNIQUE : DÉFAILLANCE HARDWARE — Critique

Les capteurs (caméras, balance) ne résistent pas aux conditions extrêmes (froid, condensation) ou manquent de précision dans la détection. En conséquence, l'utilisateur perd confiance ("Gadget inutile") et le taux de retour SAV explose, faussant l'inventaire.

En prévention :

- Sélectionner exclusivement des composants certifiés étanches et testés à -10°C.
- Implémenter un algorithme de "Sanity Check" (ex: rejeter automatiquement toute valeur de poids négative).

En réaction :

- Remplacement gratuit et immédiat du module défectueux (SAV Premium) et patch logiciel correctif.

RISQUE PLANNING : RETARD PROTOTYPE — Majeur

L'intégration Hardware/Software prend plus de temps que prévu (problèmes de drivers, PCB, approvisionnement composants). Le risque serait de décaler la phase d'industrialisation et de rater la fenêtre de lancement stratégique (Fêtes de fin d'année).

En prévention :

- Adopter une méthode Agile pour livrer des briques fonctionnelles régulièrement (MVP).
- Utiliser la marge de sécurité (15%) du budget pour renforcer l'équipe (Freelance ponctuel).

En réaction :

- Réduire le périmètre du MVP (ex: supprimer la commande vocale ou la reconnaissance d'emballage) pour tenir la date.

ANALYSE DÉTAILLÉE & PLANS D'ACTION

RISQUE JURIDIQUE : PROBLÈME DE DONNÉES (GDPR) **Majeur**

La collecte de données alimentaires jugée intrusive, ou advient une fuite de données utilisateurs du à un piratage. Dans ce cas, notre marque s'expose à de lourdes amendes (CNIL), un bad buzz médiatique et la perte définitive de l'image de marque.

En prévention :

- Architecture "Privacy by Design" : Stockage local des données sensibles ("Local First"), anonymisation lors de l'envoi cloud.
- Audit de sécurité externe (PenTest) avant le lancement.

En réaction :

- Communication de crise transparente immédiate et déploiement d'un correctif de sécurité sous 24h.

RISQUE HUMAIN : PROBLÈMES DE COMMUNICATION **Mineur**

Il faut éviter le cloisonnement entre l'équipe Hardware (IoT) et Software (App) au risque d'entraîner des spécifications mal comprises ou des incompatibilités techniques découvertes tardivement et nécessitant une refonte coûteuse.

En prévention :

- Mise en place de rituels "Daily Stand-up" communs à toute l'équipe technique.
- Utilisation d'une documentation centrale unique (Confluence/Notion).

En réaction :

- Médiation par le Chef de Projet et organisation d'ateliers de "Team Building" technique.